③

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-283554
(43)Date of publication of application : 03.10.2003

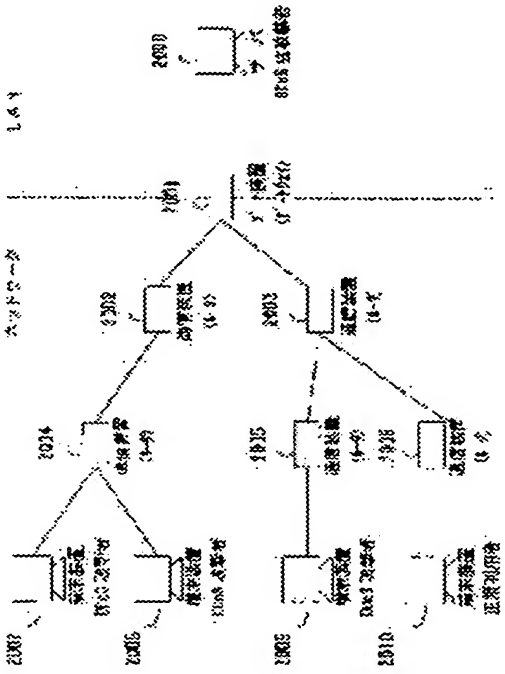
(51)Int.Cl. H04L 12/56
H04L 12/46

(21)Application number : 2002-081904
(22)Date of filing : 22.03.2002

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KASHIWA MASARU
ERIC CHEN
FUJI HITOSHI

(54) DISTRIBUTED DENIAL OF SERVICE ATTACK PREVENTING METHOD, GATE DEVICE, COMMUNICATION DEVICE, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To limit the transmission band of offensive traffic for a distributed denial of service (DDoS) attack while securing communication traffic for regular users.
SOLUTION: When the suspicious offensive packet of the DDoS attack is detected, a gate device 2001 transmits the suspicious signature and the regular condition of the suspicious offensive packet to upstream communication devices 2002 and 2003. Each of the communication devices 2002 and 2003 cancels the transmission band limitation of the packet identified from the regular condition and a regular signature created based upon the suspicious signature while limiting the transmission band of the packet identified from the suspicious signature. Further, each of the communication devices 2003 and 2003 transmits the suspicious signature and the regular condition to further upstream communication devices to report the suspicious signature and the regular condition to the upper- most stream communication device in the recursive manner and each communication device further limits the band by detecting the offensive packet from the suspicious offensive packets while implementing the band limitation of the suspicious offensive packet.



LEGAL STATUS

[Date of request for examination]	05.12.2002
[Date of sending the examiner's decision of rejection]	01.03.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3699941

[Date of registration]	15.07.2005
[Number of appeal against examiner's decision of rejection]	2005-05466
[Date of requesting appeal against examiner's decision of rejection]	31.03.2005
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－283554
（P2003－283554A）
(43)公開日　平成15年10月３日(2003.10.3)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード(参考)
Ｈ０４Ｌ　12/56	２００	Ｈ０４Ｌ　12/56	２００Ｚ　５Ｋ０３０
12/46		12/46	Ｅ　５Ｋ０３３

審査請求　有　　請求項の数14　ＯＬ　（全 18 頁）

(21)出願番号　特願2002－81904(P2002－81904)

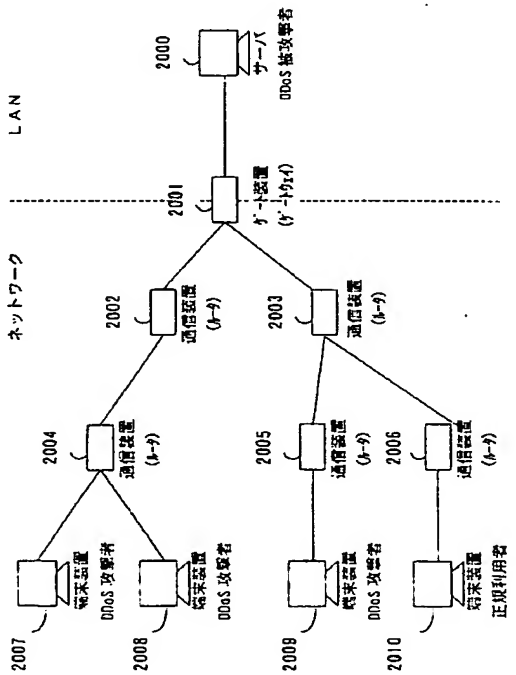
(22)出願日　平成14年３月22日(2002.3.22)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　柏　大
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　エリック・チェン
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　分散型サービス不能攻撃防止方法及びゲート装置、通信装置ならびにプログラム

(57)【要約】
【課題】　正規利用者の通信トラヒックを確保しながら、分散型サービス不能攻撃（ＤＤｏＳ攻撃）の攻撃トラヒックの伝送帯域を制限することを可能とする。
【解決手段】　ゲート装置２００１は、ＤＤｏＳ攻撃の攻撃容疑パケットを検出すると、上流の通信装置２００２、２００３に攻撃容疑パケットの容疑シグネチャと正規条件を送信する。通信装置２００２、２００３は、容疑シグネチャで識別されるパケットの伝送帯域を制限しながら、正規条件と容疑シグネチャを基に生成される正規シグネチャで識別されるパケットの伝送帯域制限を解除する。通信装置２００２、２００３はさらに上流の通信装置に容疑シグネチャと正規条件を送信することによって、最上流の通信装置まで再帰的に容疑シグネチャと正規条件を通知し、各通信装置は、攻撃容疑パケットの帯域制限を実施しながら、攻撃容疑パケットから攻撃パケットを検出して、さらに帯域を制限する。



1

【特許請求の範囲】

【請求項１】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮと、前記ＬＡＮおよびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、

前記ゲート装置は、

通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックし、

合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成して上流の前記通信装置へ送信し、

以後、前記容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行い、

前記通信装置は、

下流のゲート装置または通信装置から受信した前記容疑シグネチャを上流の通信装置へ送信すると共に、前記容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行うことを特徴とする分散型サービス不能攻撃防止方法。

【請求項２】　前記ゲート装置及び前記通信装置は、前記容疑シグネチャで識別される攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出し、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、以後前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限する処理を行うことを特徴とする請求項１に記載の分散型サービス不能攻撃防止方法。

【請求項３】　前記ゲート装置は、正規利用者の端末装置からの通信パケットの条件である予め決められた正規条件を上流の通信装置へ送信すると共に、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、

以後、前記正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行い、

前記通信装置は、下流のゲート装置または通信装置から受信した前記正規条件を上流の通信装置へ送信すると共に、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、

以後、正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行うことを特徴とする請求項１または請求項２に記載の分散型サービス不能攻撃防止方法。

【請求項４】　アクティブネットワーク上で動作することを特徴とする請求項１～請求項３のいずれかの項に記載の分散型サービス不能攻撃防止方法。

【請求項５】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置において、

分散型サービス不能攻撃の攻撃容疑パケットの検出条件を記憶するパケット検出条件記憶部と、

入力される通信パケットをチェックし、前記パケット検出条件記憶部が記憶する攻撃容疑パケットの検出条件を基に攻撃容疑パケットの発生を検出するトラヒック監視手段と、

前記トラヒック監視手段によって検出された前記攻撃容疑パケットの伝送帯域を制限する帯域制御手段と、

前記攻撃容疑パケットの検出条件を基に前記攻撃容疑パケットを識別する容疑シグネチャを生成するシグネチャ生成手段と、

前記容疑シグネチャを上流の通信装置に対して送信するシグネチャ送信手段と、

を備えることを特徴とするゲート装置。

【請求項６】　前記トラヒック監視手段は、入力される前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出し、

前記帯域制御手段は、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限することを特徴とする請求項５に記載のゲート装置。

【請求項７】　前記パケット検出条件記憶部は、さらに、通信パケットが正規利用者の端末装置からの通信パケットである条件を示す正規条件を記憶し、

前記シグネチャ生成手段は、前記容疑シグネチャと前記正規条件とを基に正規パケットを識別する正規シグネチャを生成し、

前記帯域制御手段は、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除し、

前記シグネチャ送信手段は、前記正規条件を前記上流の通信装置に対して送信することを特徴とする請求項５または請求項６に記載のゲート装置。

【請求項８】　防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置において、

下流のゲート装置あるいは通信装置から容疑シグネチャを受信するシグネチャ受信手段と、

前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限する帯域制御手段と、

前記容疑シグネチャを上流の通信装置に送信するシグネチャ送信手段と、

を備えることを特徴とする通信装置。

【請求項９】　入力される前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するトラヒック監視手段を備え、

前記帯域制御手段は、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限することを特徴とする請求項８に記載の通信装置。

【請求項１０】　前記シグネチャ受信手段は、前記下流のゲート装置あるいは通信装置から正規条件を受信し、前記帯域制御手段は、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除し、

前記シグネチャ送信手段は、前記正規条件を前記上流の通信装置に送信することを特徴とする請求項８または請求項９に記載の通信装置。

【請求項１１】　複数の通信装置を網目状に接続してなるネットワークと、

防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムであって、

入力される通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックするステップと、

合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成するステップと、

予め決められた正規条件と前記容疑シグネチャを基に正規パケットを識別する正規シグネチャを生成するステップと、

前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、

前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、

前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、

前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、

前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、

をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

【請求項１２】　防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置上で実行されるコンピュータプログラムであって、

下流のゲート装置あるいは通信装置から容疑シグネチャと正規条件とを受信するステップと、

前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、

前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを作成し、作成された前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、

前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、

前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、

前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、

をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラム。

【請求項１３】　複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、

入力される通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックするステップと、

合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成するステップと、

予め決められた正規条件と前記容疑シグネチャを基に正規パケットを識別する正規シグネチャを生成するステップと、

前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、

前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、

前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、

前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、

前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、

の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【請求項１４】　防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置上で実行されるコンピュータプログラムであって、

下流のゲート装置あるいは通信装置から容疑シグネチャと正規条件とを受信するステップと、

前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、

前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、

5

前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、
前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、
前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、
の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークに接続された機器をネットワーク経由での攻撃から防御するための、分散型サービス不能攻撃の防止方法およびその装置ならびにそのコンピュータプログラムに関するものである。

【０００２】

【従来の技術】従来、ＴＣＰ／ＩＰ（Transmission control protocol/internet protocol）などのネットワークプロトコルは、オープンとなっており、互いに信用されるグループで使われるように設計されている。このため、コンピュータのオペレーティングシステムでは、大量の通信トラフィック（データ等）を攻撃目標のサーバに送信することによって、ネットワークの伝送帯域やサーバの資源を消費して正当な利用者の利用を妨げようとするサービス不能攻撃（以下、「ＤｏＳ（Denialof Service）攻撃」と記す）を防ぐことは考慮されていない。このようなＤｏＳ攻撃に対する防御の方法は増えてきているが、複数箇所から同時に連携してＤｏＳ攻撃を行う「ＤＤｏＳ（Distributed Denial of Service）攻撃」に対する防御の方法は未だ効果的な方法が開発されていない。

【０００３】このＤＤｏＳ攻撃に対する防御の方法としては、シスコ社が提案したＩｎｇｒｅｓｓ Ｆｉｌｔｅｒ（ＲＦＣ２２６７）とＵＵＮＥＴ社のＣｅｎｔｅｒ Ｔｒａｃｋがある。前者は、ＤＤｏＳ攻撃の際に良く使われる送信元アドレスの詐称をチェックする機構であり、ローカルエリアネットワークがインターネットに接続されている境界であるルータにインストールされ、ローカルエリアネットワークからインターネットに向かって送信されるパケットの送信元アドレスの正統性をチェックし、ローカルエリアネットワークに割り当てられたアドレスと整合していない場合には、そのパケットをインターネットに送信せずに破棄する。一方後者は、インターネットのルータに診断機能を付加し、ＤＤｏＳ攻撃の送信元を追跡する技術である。

【０００４】また、ＤＤｏＳ攻撃を検出したノードより攻撃元に近い上流ノードで攻撃トラヒックを制限するための技術としては、本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法（特願２００１－２７４０１６）、ＡＴ＆Ｔ社論文（R.Mahajan, S.M.Bellovin, S.Floyd, J.Ioannidis, V.Paxson and S.Shenker: "Controlling high bandwidth aggregates in the network - extended version" (2001)）、ＩＤＩＰ（Intruder Detection and Isolation Protocol）（D.Schnackenberg, K.Djahandari and D.Sterne: "Infrastructure for intrusion detection and response", Proceedings of the DARPA Information Survivability Conference and Exposition(DISCEX), South Carolina(2000)）などがある。ＡＴ＆Ｔ社論文及びＩＤＩＰは、攻撃検出イベントを攻撃経路の上流ノードへ伝達し、上流ノードで伝送帯域制限を行うための方式やプロトコルである。本出願の発明者等が出願済みの分散型サービス不能攻撃の防止方法は、ルータにインストールされている移動型パケットフィルタリングプログラムが、自らのプログラムの複製を作成し、その複製を上流ルータ移動させ、各上流ルータへ移動してきた移動型パケットフィルタリングプログラムは、それぞれＤＤｏＳ攻撃者のホストから攻撃目標のサーバに向けて送られているトラフィック全てを通過させないようする技術である。

6

【０００５】

【発明が解決しようとする課題】上述したＩｎｇｒｅｓｓ Ｆｉｌｔｅｒ（ＲＦＣ２２６７）は、送信元アドレスを詐称してＤＤｏＳ攻撃をすることを禁止するための技術であり、攻撃を受ける側が防御するために使う技術ではない。また、Ｃｅｎｔｅｒ Ｔｒａｃｋは、攻撃を受けた被害者が攻撃者を特定することを助ける技術ではあるが、実際に攻撃を受けているときにその攻撃を防御することはできない。

【０００６】さらに、上述したＩｎｇｒｅｓｓ Ｆｉｌｅｔｅｒ（ＲＦＣ２２６７）は、正しいＩＰ（internet protocol）アドレスが送信元になっているＩＰパケットによる攻撃にはまったく対処できない、攻撃元になっているローカルエリアネットワークとインターネットとの境界であるルータにＩｎｇｒｅｓｓ Ｆｉｌｔｅｒが具備されていない場合はまったく攻撃の防御に役に立たないという問題点がある。また、上述したＣｅｎｔｅｒ Ｔｒａｃｋは、複数箇所に分散された分散型ＤｏＳの攻撃元になっているコンピュータやそのコンピュータが接続されているネットワークの管理者に連絡をしないと、攻撃そのものを止めることはできないため、実質的には攻撃を止めるまでに何時間、あるいは何日もの時間がかかってしまうという問題点がる。

【０００７】また、この出願の同発明者等が出願済みの分散型サービス不能攻撃の防止方法やＡＴ＆Ｔ論文では、ＩＰパケットのデータフィールドやパケットの宛先情報など、決められた属性のみで攻撃パケットを特定するため、被攻撃者の要求する攻撃属性を反映できないと

いう問題がある。さらに、これらの分散型サービス不能攻撃の防止方法、ＡＴ＆Ｔ論文及びＩＤＩＰにおては、攻撃パケットと特定されたパケットを次ノードへ送出せず、全て破棄してまう。よって、標的となるサーバのダウンやルータ装置の過負荷等によりサービスが停止する一次被害を防止することはできるが、正規利用者からのパケットを攻撃パケットと識別する方法がないため、誤って正規利用者からの正規パケットも攻撃パケットとして破棄してしまう可能性があり、正規利用者の利用性が低下するといった二次被害を引き起こしてしまうという問題がある。

【０００８】本発明は、上記事情を考慮してなされたものであり、その目的は、正規利用者へのサービス性を低下させる被害を軽減しながら上流ノードでＤＤｏＳ攻撃を防御できる、分散型サービス不能攻撃防止方法及び装置ならびにプログラムを提供することにある。

【０００９】

【課題を解決するための手段】この発明は、上記の課題を解決すべくなされたもので、請求項１に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮと、前記ＬＡＮおよびネットワークの間に介挿されたゲート装置とを有するネットワークシステムにおいて、前記ゲート装置は、通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックし、合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成して上流の前記通信装置へ送信し、以後、前記容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行い、前記通信装置は、下流のゲート装置または通信装置から受信した前記容疑シグネチャを上流の通信装置へ送信すると共に、前記容疑シグネチャによって識別される攻撃容疑パケットの伝送帯域を制限する処理を行うことを特徴とする分散型サービス不能攻撃防止方法である。

【００１０】請求項２に記載の発明は、請求項１に記載の分散型サービス不能攻撃防止方法であって、前記ゲート装置及び前記通信装置は、前記容疑シグネチャで識別される攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出し、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、以後前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限する処理を行うことを特徴とする。

【００１１】請求項３に記載の発明は、請求項１または請求項２に記載の分散型サービス不能攻撃防止方法であって、前記ゲート装置は、正規利用者の端末装置からの通信パケットの条件である予め決められた正規条件を上流の通信装置へ送信すると共に、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、以後、前記正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行い、前記通信装置は、下流のゲート装置または通信装置から受信した前記正規条件を上流の通信装置へ送信すると共に、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、以後、前記正規シグネチャによって識別される正規パケットの伝送帯域制限を解除する処理を行うことを特徴とする。

【００１２】請求項４に記載の発明は、請求項１～請求項３のいずれかの項に記載の分散型サービス不能攻撃防止方法であって、アクティブネットワーク上で動作することを特徴とする。

【００１３】請求項５に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置において、分散型サービス不能攻撃の攻撃容疑パケットの検出条件を記憶するパケット検出条件記憶部と、入力される通信パケットをチェックし、前記パケット検出条件記憶部が記憶する攻撃容疑パケットの検出条件を基に攻撃容疑パケットの発生を検出するトラヒック監視手段と、前記トラヒック監視手段によって検出された前記攻撃容疑パケットの伝送帯域を制限する帯域制御手段と、前記攻撃容疑パケットの検出条件を基に前記攻撃容疑パケットを識別する容疑シグネチャを生成するシグネチャ生成手段と、前記容疑シグネチャを上流の通信装置に対して送信するシグネチャ送信手段と、を備えることを特徴とするゲート装置である。

【００１４】請求項６に記載の発明は、請求項５に記載のゲート装置であって、前記トラヒック監視手段は、入力される前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出し、前記帯域制御手段は、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限することを特徴とする。

【００１５】請求項７に記載の発明は、請求項５または請求項６に記載のゲート装置であって、前記パケット検出条件記憶部は、さらに、通信パケットが正規利用者の端末装置からの通信パケットである条件を示す正規条件を記憶し、前記シグネチャ生成手段は、前記容疑シグネチャと前記正規条件とを基に正規パケットを識別する正規シグネチャを生成し、前記帯域制御手段は、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除し、前記シグネチャ送信手段は、前記正規条件を前記上流の通信装置に対して送信することを特徴とする。

【００１６】請求項８に記載の発明は、防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置において、下流のゲート装置あるいは通信装置から容疑シグネチャを受信するシグネチャ受信手段と、前記容疑シグネチャで識別

される攻撃容疑パケットの伝送帯域を制限する帯域制御手段と、前記容疑シグネチャを上流の通信装置に送信するシグネチャ送信手段と、を備えることを特徴とする通信装置である。

【００１７】請求項９に記載の発明は、請求項８に記載の通信装置であって、入力される前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するトラヒック監視手段を備え、前記帯域制御手段は、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定して、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限することを特徴とする。

【００１８】請求項１０に記載の発明は、請求項８または請求項９に記載の通信装置であって、前記シグネチャ受信手段は、前記下流のゲート装置あるいは通信装置から正規条件を受信し、前記帯域制御手段は、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除し、前記シグネチャ送信手段は、前記正規シグネチャを前記下流の通信装置に送信することを特徴とする。

【００１９】請求項１１に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムであって、入力される通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックするステップと、合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成するステップと、予め決められた正規条件と前記容疑シグネチャを基に正規パケットを識別する正規シグネチャを生成するステップと、前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【００２０】請求項１２に記載の発明は、防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置上で実行されるコンピュータプログラムであって、下流のゲート装置あるいは通信装置から容疑シグネチャと正規条件とを受信するステップと、前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを作成し、作成された前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、をコンピュータに実行させることを特徴とする分散型サービス不能攻撃防止プログラムである。

【００２１】請求項１３に記載の発明は、複数の通信装置を網目状に接続してなるネットワークと、防御対象であるコンピュータおよびＬＡＮとの間に介挿されたゲート装置上で実行されるコンピュータプログラムを記録したコンピュータ読み取り可能な記録媒体であって、入力される通信トラヒックが予め決められた攻撃容疑パケットの検出条件に合致するか否かをチェックするステップと、合致したトラヒックを検出した場合に、検出された前記攻撃容疑パケットを識別する容疑シグネチャを生成するステップと、予め決められた正規条件と前記容疑シグネチャを基に正規パケットを識別する正規シグネチャを生成するステップと、前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送出される攻撃パケットの伝送帯域をさらに制限するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体である。

【００２２】請求項１４に記載の発明は、防御対象であるコンピュータおよびＬＡＮがゲート装置を介して接続されたネットワークを構成する通信装置上で実行されるコンピュータプログラムであって、下流のゲート装置あるいは通信装置から容疑シグネチャと正規条件とを受信するステップと、前記容疑シグネチャで識別される攻撃容疑パケットの伝送帯域を制限するステップと、前記正規条件と前記容疑シグネチャとを基に正規パケットを識別する正規シグネチャを生成し、前記正規シグネチャで識別される正規パケットの伝送帯域制限を解除するステップと、前記容疑シグネチャと前記正規条件を上流の通信装置に送信するステップと、前記攻撃容疑パケットのトラヒックを分析して攻撃トラヒックを検出するステップと、前記攻撃トラヒックを構成するパケットの送出元ネットワークを特定し、前記送出元ネットワークから送

出される攻撃パケットの伝送帯域をさらに制限するステップと、の各処理をコンピュータに実行させる分散型サービス不能攻撃防止プログラムを記録することを特徴とする記録媒体である。

【００２３】

【発明の実施の形態】以下図面を参照し、この発明の一実施の形態について説明する。図１は、同実施の形態を適用したネットワークの構成図である。この図において、２０００はサーバ、２００１はこの発明の一実施形態によるゲート装置（ゲートウェイ）、２００２～２００６はこの発明の一実施形態による通信装置（ルータ）、２００７～２０１０は端末装置である。ＤＤｏＳ攻撃の被攻撃者のサーバ２０００が収容されているＬＡＮ（ローカルエリアネットワーク）は、ゲート装置２００１によって外部のネットワークに接続されている。そして、ネットワークは通信装置２００２、２００３、２００４、２００５、２００６を有している。ＤＤｏＳ攻撃者によって操作された端末装置２００７、２００８、２００９が、攻撃パケットを被攻撃者のサーバ２０００に向かって送信すると、攻撃パケットが被攻撃者収容ＬＡＮに集中して混雑が発生することにより、ゲート装置２００１の資源を消費してしまい、ＤＤｏＳ攻撃者とは無関係な正規利用者の端末２０１０からサーバ２０００に接続できなくなるという現象が起こる。

【００２４】ゲート装置２００１は、予めサーバ２０００を保有する利用者が設定した攻撃容疑検出条件及び正規条件を記憶している。図２に攻撃容疑検出条件の設定の例を、図３に正規条件の設定の例を示す。さらに、ゲート装置２００１は、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値を記憶している。

【００２５】図２における攻撃容疑検出条件は、検出属性、検出閾値及び検出間隔の組からなる３組のレコードで構成される。ここでは、番号はレコードを特定するために便宜上使用される。攻撃容疑検出条件は、受信パケットが攻撃パケットである可能性がある攻撃容疑パケットを検出するために使用され、３組のレコードの内のいずれかのレコードの条件にトラヒックが一致した場合、このトラヒックの通信パケットは攻撃容疑パケットであると認識される。検出属性は、ＩＰパケットの第３／４層属性種別とそれら属性値の組を指定するが、第３層属性であるＩＰの「Destination IP Address（宛先ＩＰアドレス）」という属性種別は必ず指定される。図２において、番号１のレコードの検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.1/32」であり（dst=192.168.1.1/32）、ＩＰの上位層（第４層）のプロトコル種別を示す「Protocol（プロトコル）」が「ＴＣＰ」であり（Protocol=TCP）、かつ、第４層プロトコルがどのアプリケーションの情報かを示す「Destination Port（宛先ポート番号）」が「８０」で

ある（Port=80）という属性種別とそれら属性値の組で指定される。番号２のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.2/32」であり（dst=192.168.1.2/32）、かつ、「Protocol（プロトコル）」が「ＵＤＰ（User Datagram protocol）」である（Protocol=UDP）という属性種別とそれら属性値の組で指定される。また、番号３のレコード検出属性は、「Destination IP Address（宛先ＩＰアドレス）」が「192.168.1.0/24」である属性種別とその属性値で指定される。検出閾値は、同じレコードで指定される検出属性を持つ受信パケットのトラヒックを攻撃容疑トラヒックとして検出するための最低の伝送帯域を、検出間隔は同じく最低の連続時間を示している。

【００２６】図３における正規条件は、ＩＰパケットの第３／４層属性種別とそれら属性値の組からなる複数のレコードで構成される。ここでは、番号はレコードを特定するために便宜上使用される。正規条件は、受信パケットが正規利用者の端末装置からのパケットである、すなわち正規パケットである条件であり、たとえ、図２の攻撃容疑検出条件に合致したパケットであっても、正規条件に合致する場合は正規パケットと判断される。図３において、番号１のレコードの検出属性は、ＩＰの「Source IP Address（送信元ＩＰアドレス）」が「172.16.10.0/24」であることを指定し（src=172.16.10.0/24）、番号２のレコードの検出属性はＩＰ上のサービス品質を示す「Type of Service（サービスタイプ）」が「０１（ヘキサ）」であることを指定している（TOS=0x01）。この正規条件には、例えば、サーバ所有者の会社の支店や、関連会社など、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者が正規ユーザであると認識しているネットワークの送信元ＩＰアドレスなどが設定される。

【００２７】また、ゲート装置２００１及び通信装置２００２～２００６は、攻撃容疑パケットのトラヒックを分析し、不正トラヒックを検出するための不正トラヒック検出条件を保有する。図４に不正トラヒック検出条件の設定の例を示す。ここでは、番号はレコードを特定するために便宜上使用される。不正トラヒック条件は、既知のＤＤｏＳ攻撃の複数のトラヒックパターンから構成され、攻撃容疑パケットのトラヒックがいずれかのトラヒックパターンに合致した場合に、不正トラヒックであると認識される。図４の番号１の不正トラヒック条件は、「伝送帯域Ｔ１Ｋｂｐｓ以上のパケットがＳ１秒以上連続送信されている」というトラヒックパターンを示している。また、番号２の不正トラヒック条件は、「伝送帯域Ｔ２Ｋｂｐｓ以上、第３層プロトコルであるＩＣＭＰ（Internet Control Message Protocol）上のエコー応答（Echo Reply）メッセージのパケットがＳ２秒以上連続送信されている」というトラヒックパターンを示している。番号３の不正トラヒック条件は、「伝送帯域

Ｔ３Ｋｂｐｓ以上、データが長すぎるためパケットに含まれるデータは複数ＩＰパケットに分割して送信していることを示すフラグメントパケットがＳ３秒以上連続送信されている」というトラヒックパターンを示している。

【００２８】ここで、ゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルを説明する。図５は本実施の形態におけるゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルを示す。帯域制御モデルは、入力パケットをクラス別に分類し、このクラスに従ってパケットの出力帯域制御を実現するためのモデルを示す。フィルタ２０２１は、入力されたパケットを正規クラス２０２２、容疑クラス２０２６、不正クラス２０２４の３つのクラスに分類する。なお、このフィルタ２０２１の分類アルゴリズムは後述する。正規クラス２０２２はデフォルトクラスであり、正規クラス２０２２に分類されたパケットは正規キュー２０２３につながれ、伝送帯域を制限せずに出力される。容疑クラス２０２６に分類されたパケットは、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮ毎に発生する容疑キュー２０２７につながれ、防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値に出力伝送帯域が制限される。サーバ２０００を収容しているゲート装置２００１の容疑キューの伝送帯域制限値は防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値を使用するが、上流の通信装置２００２～２００６では、下流のルータから受信した伝送帯域制限値を使用する。なお、容疑シグネチャの生成については後述する。不正クラス２０２４に分類されたパケットは、不正キュー２０２５につながれ、サーバ所有者やネットワークのポリシーに関わらず、０または０に近い伝送帯域に制限される。

【００２９】続いて、ゲート装置２００１及び通信装置２００２～２００６が伝送帯域制限を実行するための、フィルタ２０２１の分類アルゴリズムについて説明する。ゲート装置２００１及び通信装置２００２～２００６は、入力される全ての通信パケットをこの分類アルゴリズムで分類する。

【００３０】図６はフィルタ２０２１における分類アルゴリズムを示す。まず、ステップＳ３００１において、フィルタ２０２１は、入力されたパケットが正規シグネチャに合致するか判断する。正規シグネチャに合致した場合には、パケットは正規クラス２０２２に分類される（ステップＳ３００２）。ここで、正規シグネチャに合致しなかった場合はステップＳ３００３に進み、パケットが不正シグネチャと合致するか判断する。不正シグネチャに合致した場合、パケットは不正クラス２０２４に分類される（ステップＳ３００４）。不正シグネチャに合致しなかった場合はステップＳ３００５に進み、パケットが容疑シグネチャであるか判断し、容疑シグネチャに合致すれば容疑クラス２０２６へ分類され（ステップＳ３００６）、容疑シグネチャに合致しない、すなわち全てのシグネチャに合致しない場合には正規クラス２０２２へ分類される（ステップＳ３００７）。このようにして各クラスに分類されたパケットは、正規キューであれば伝送帯域制限せずに出力され、容疑キュー及び不正キューであればそれぞれの伝送帯域制限値に従って伝送帯域が制限されて出力される。なお、正規シグネチャ、容疑シグネチャ及び不正シグネチャの生成については後述する。

【００３１】次に、図７のゲート装置２００１の攻撃容疑パケット検出時の動作を示すフローチャート、図８の通信装置２００２、２００３のシグネチャ受信時の動作を示すフローチャート及び図９のゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を示すフローチャートを使用して、ＤＤｏＳ攻撃対策方式の処理手順を示す。

【００３２】図７のステップＳ３０１１において、ゲート装置２００１は、攻撃容疑検出条件（図２）に従って、検出間隔で指定されているより長い時間連続して、検出閾値で指定されている以上の伝送帯域を使用している、検出属性に合致するトラヒックをチェックし、３組のレコードの内のいずれかのレコードに合致した場合、このトラヒックを攻撃容疑トラヒックとして検出する。すると、ステップＳ３０１２において、この検出された攻撃容疑トラヒックが満たしている攻撃容疑検出条件のレコードの検出属性を、容疑シグネチャとして生成する。容疑シグネチャは、攻撃容疑トラヒックの通信パケット、すなわち攻撃容疑パケットを識別する。さらに、正規条件（図３）を参照し、正規条件の全てのレコード毎にこの容疑シグネチャとＡＮＤ条件をとり、これを正規シグネチャとして生成する。正規シグネチャは、容疑シグネチャから正規ユーザの通信パケットである正規パケットを識別するために用いられる。例えば、図２と図３の設定例を用いて説明すると、図２における番号１のレコードの条件で検出されるパケットの容疑シグネチャは{dst=192.168.1.1/32, Protocol=TCP, Port=80}となり、図３より正規シグネチャは{src=172.16.10.24, dst=192.168.1.1/32, Protocol=TCP, Port=80}及び{TOS=0x01, dst=192.168.1.1/32, Protocol=TCP, Port=80}となる。

【００３３】次いで、ステップＳ３０１３において、ゲート装置２００１は、ステップＳ３０１２において生成した容疑シグネチャ及び正規シグネチャをフィルタ２０２１に登録し、攻撃容疑トラヒックを防御対象のサーバ２０００及びサーバ２０００が収容されているＬＡＮの所有者によって予め設定された伝送帯域制限値に伝送帯域を制限するための容疑キュー２０２７を生成する。

尚、同一防御対象に関する容疑キューが既に生成済みの場合は、新たな容疑キューの生成は行わない。これにより、図５に示す帯域制御モデルと図６に示すフィルタ２０２１の分類アルゴリズムに従って、容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限と、正規シグネチャに合致する正規パケットの伝送帯域制限の解除が実行される。

【００３４】そして、ゲート装置２００１は、ステップＳ３０１４を実行する。すなわち、ゲート装置２００１は、容疑シグネチャと正規条件と攻撃容疑パケットの帯域制限値とを上流の通信装置２００２、２００３に送信する。ここで送信する攻撃容疑パケットのトラヒックの帯域制限値は、例えば、ゲート装置２００１が記憶する攻撃容疑検出条件のレコードに対応したの伝送帯域制限値を上流の通信装置全てに均等に分配するなどの方法で算出される。

【００３５】次に、容疑シグネチャ、正規条件及び攻撃容疑パケットの帯域制限値の受信時の通信装置２００２、２００３の動作を説明する。図８のステップＳ３０２１において、通信装置２００２、２００３は、ゲート装置２００１が送信した（ステップＳ３０１４）容疑シグネチャと正規条件と容疑パケットの帯域制限値とを受信する。すると、ステップＳ３０２２において、通信装置２００２、２００３は、受信した容疑シグネチャと正規条件を基に正規シグネチャを生成する。すなわち、正規シグネチャは、受信した正規条件の全てのレコード毎に、受信した容疑シグネチャとＡＮＤ条件をとり、これを正規シグネチャとして生成する。次に、ステップＳ３０２３に進み、通信装置２００２、２００３は、受信した容疑シグネチャ及び算出した正規シグネチャをフィルタ２０２１に登録し、容疑シグネチャ及び攻撃容疑パケットのトラヒックの伝送帯域制限値に対応した容疑キュー２０２７を生成する。これにより、図５に示す帯域制御モデルと図６に示すフィルタ２０２１の分類アルゴリズムに従って、容疑シグネチャに合致する攻撃容疑パケットの伝送帯域の制限と、正規シグネチャに合致する正規パケットの伝送帯域制限の解除が実行される。そして、ステップＳ３０２４において、通信装置２００２はその上流にある通信装置２００４に、通信装置２００３はその上流にある通信装置２００５及び２００６に受信した容疑シグネチャと正規条件及び受信した伝送帯域制限値より小さい攻撃容疑パケットの伝送帯域制限値を送信する。ここで攻撃容疑パケットの伝送帯域制限値は、例えば、通信装置２００２、２００３が受信した伝送帯域制限値を上流の通信装置全てに均等に分配するなどの方法で算出される。

【００３６】そして、通信装置２００４～２００６は、通信装置２００２、２００３から容疑シグネチャと正規条件及び攻撃容疑パケットの伝送帯域制限値を受信し、通信装置２００２、２００３におけるステップＳ３０２１～Ｓ３０２３と同様に動作する。

【００３７】次に、ゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を説明する。図９のステップＳ３０３１において、ゲート装置２００１及び通信装置２００２～２００６は、ＤＤｏＳ攻撃者がパケットを送出しているネットワークを特定するため入力パケットを分析して、不正トラヒック条件（図４）のいずれかのパターンに合致するトラヒックを検出する。すると、ゲート装置２００１及び通信装置２００２～２００６は、ステップＳ３０３２において、この検出された不正トラヒック条件（図４）を満たすパケットの送信元ＩＰアドレスを不正アドレス範囲として特定し、この不正アドレス範囲であり、かつ、容疑シグネチャに合致するという条件を不正シグネチャとする。そしてゲート装置２００１及び通信装置２００２～２００６は、ステップＳ３０３３においてこの不正シグネチャをフィルタ２０２１に登録する。これにより、図５に示す帯域制御モデルと図６に示すフィルタ２０２１の分類アルゴリズムに従って、不正シグネチャで識別される攻撃パケットの伝送帯域はさらに制限される。

【００３８】ところで、以上説明した動作は、以下に記述するアクティブネットワーク上で実行される。

【００３９】以下、図面を参照しこの発明の一実施形態を実行できるアクティブネットワークについて説明する。図１０は、本実施形態が前提とするネットワークの構成である。図１０に示すように、通信ネットワークは、複数の通信装置７００１によって接続されている。そして、通信装置７００１には１台または複数台のユーザのコンピュータ７０００を接続することができるようになっている。ユーザのコンピュータ７０００相互間で通信データのやりとりを行う際には、送信元のユーザのコンピュータ７０００が送信したパケットを通信ネットワーク上の各ノードに位置する通信装置７００１が順次転送することにより、そのパケットを宛先のユーザのコンピュータ７０００に届けるようにする。

【００４０】次に、通信装置の構成について説明する。図１１は、通信装置７００１の内部の構成を示すブロック図である。図１１に示すように、通信装置７００１には通信線７０２４ａ、７０２４ｂ、７０２４ｃ、７０２４ｄが接続されており、通信装置７００１はこれらの通信線を介して隣接する他の通信装置との間でパケットを交換することができるようになっている。また、通信装置７００１には、上記の各通信線７０２４ａ～７０２４ｄに対応したインタフェース部７０２３ａ～７０２３ｄと、パケットを転送する処理を行うための転送処理部７０２１と、パケットの転送の際の転送先の情報を記憶する転送先テーブル７０２２と、アクティブパケットに対する処理を行うためのアクティブネットワーク実行環境（ActiveNetwork Execution Environment）７０１０とが設けられている。なお、アクティブネットワーク実行

17

環境７０１０は、内部に、アクティブコード（プログラム）を実行するためのコード実行部７０１１と、アクティブコードを記憶しておくためのコード記憶部７０１２とを備えている。なお、ここでアクティブコードとは、アクティブネットワークにおいてパケットに対する作用を行うコンピュータプログラムのコードである。

【００４１】ここで、図１１を参照しながら、この通信装置７００１の動作例の概要を説明する。隣接する他の通信装置から通信線７０２４ｄを介してパケットが到着すると、インタフェース部７０２３ｄがそのパケットを受信し転送処理部７０２１に渡す。転送処理部７０２１は、渡されたパケットのヘッダ部分に格納されている送信元（source）アドレスと宛先（destination）アドレスとを読み取り、さらにそれらのアドレスをキーとして転送先テーブル記憶部７０２２に記憶されている転送先テーブルを参照することによって、そのパケットにどう対処するかを決定する。

【００４２】パケットへの対処は大きく２通りに分けられる。そのパケットに対してアクティブコードを適用する場合と、そのパケットをそのまま他の通信装置に転送する場合とである。転送先テーブルを参照した結果、そのパケットに対してアクティブコードを適用すべきものである場合には、転送処理部７０２１は、そのパケットをアクティブネットワーク実行環境７０１０に渡す。アクティブネットワーク実行環境７０１０においては、コード実行部７０１１がそのパケットを受け取り、そのパケットに対して適用すべきアクティブコードをコード記憶部７０１２から読み出して実行する。なお、コード実行部７０１１は、アクティブコードを実行した結果、必要な場合には処理対象となったパケットを再び転送処理部７０２１に渡して他の通信装置に対して転送することもある。転送先テーブルを参照した結果、そのパケットにアクティブコードを適用せずそのまま他の転送装置に転送するべきものである場合には、転送処理部７０２１は、適切な転送先に対応したインタフェース部（７０２３ａや７０２３ｂや７０２３ｃなど）に渡し、そのインタフェース部が通信線（７０２４ａや７０２４ｂや７０２４ｃなど）を介してパケットを他の通信装置に転送する。

【００４３】なお、ここでは通信線７０２４ｄを介して他の通信装置からパケットが到着した場合を例として説明したが、他の通信線を介してパケットが到着した場合の処理も同様である。

【００４４】次に、通信装置７００１内の転送処理部７０２１がいかにしてパケットに対する処置（アクティブコードを適用するか、単純に他の通信装置に転送するか）を決定するかを具体的に説明する。

【００４５】本実施形態が基礎とするフレームワークでは、アクティブネットワーク実行環境はパケットの中において指定されているＩＰアドレスに基づいて起動される。ここで、全ての（グローバル）ＩＰアドレスの集合をＩと表わすものとする。また、送信元ＩＰアドレスがｓであり宛先ＩＰアドレスがｄであるようなパケットを（ｓ，ｄ）と表わすものとする。また、通信装置のアクティブネットワーク実行環境に格納されているすべてのアクティブコードはそれぞれ特定のユーザに属するものとし、ある特定のユーザの所有するＩＰアドレスの集合をＯと表わすものとする。

18

【００４６】本フレームワークでは、上記特定のユーザに属する個々のアクティブコードは、次に示す式による集合Ａで表されるパケットであって、かつ当該アクティブネットワーク実行環境を備えた通信装置（ノード）によって受信されたパケットに対してアクセスする権限を持つ。すなわち、

$$A = \{(s, d) \in [(O \times I) \cup (I \times O)] \mid s \neq d\}$$

である。つまり、この式が意味するところの概略は、特定のユーザに属するアクティブコードは、当該ユーザが所有する全てのＩＰアドレスのいずれかを送信元または宛先のアドレスとするようなパケットに対してアクセス権を有するということである。

【００４７】当該ユーザに属するｎ個のアクティブコードがある通信装置（ノード）に格納されているとき、ｉ番目（$1 \leqq i \leqq n$）のアクティブコードは、集合Ｃ（ｉ）（Ｃ（ｉ）$\subseteq$Ａ）に属するパケットをキャプチャーして処理することをアクティブネットワーク実行環境に対して予め要求しておく。つまり、当該ユーザに関して、アクティブネットワーク実行環境は、ｃ（１）∪ｃ（２）∪・・・・・∪ｃ（ｎ）なる和集合の要素であるパケット（ｓ，ｄ）によって起動されるものであり、このようなパケットを「アクティブパケット」と呼ぶことができる。

【００４８】図１２は、図１１に示した転送先テーブル記憶部７０２２に記憶されている転送先テーブルの一例を示す概略図である。上記のフレームワークを実現するために必要な情報は、このような転送先テーブルに格納することが可能である。

【００４９】図１２に示すように、転送先テーブルは、タイプ（Type）と宛先アドレス（Destination）と送信元アドレス（Source）と転送先（Send to）の各項目を含んでいる。タイプの項目は、テーブルのエントリーのタイプを表わすものであり、「アクティブ（Active）」あるいは「通常（Regular）」のいずれかの値をとる。宛先アドレスおよび送信元アドレスの項目は、転送対象のパケットの宛先ＩＰアドレスおよび送信元ＩＰアドレスにそれぞれ対応するものである。転送先の項目はは、宛先アドレスと送信元アドレスの組み合せがマッチしたパケットに関して、適用すべきアクティブコードの識別情報あるいは転送先の通信装置のＩＰアドレスを表わすものである。

19

【００５０】タイプの値が「アクティブ」であるエントリーは、対象のパケットに適用するアクティブコードを指定するものであり、その転送先の項目にはアクティブコードを識別する情報が書かれている。タイプの値が「通常」であるエントリーは、対象のパケットの転送先の通信装置のアドレスを指定するものであり、その転送先の項目には転送先の通信装置のＩＰアドレスが書かれている。

【００５１】図１２に示す転送先テーブルの例において、第１のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１．２．３．４」であり、送信元アドレスが「Ａｎｙ（何でもよい）」であり、転送先が「アクティブコードＡ」となっている。これは、送信元アドレスがいかなるアドレスであっても、宛先アドレスが「１．２．３．４」にマッチする場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＡが実行されることを表わしている。また、第２のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１０．５０．０．０」であり、送信元アドレスが「１１．１２．１３．１４」であり、転送先が「アクティブコードＢ」となっている。これは、宛先アドレスと送信元アドレスの両方がそれぞれ上記の値にマッチした場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＢが実行されることを表わしている。また、第３のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「Ａｎｙ（何でもよい）」であり、送信元アドレスが「１５７．２．３．０」であり、転送先が「アクティブコードＣ」となっている。これは、宛先アドレスがいかなるアドレスであっても、送信元アドレスが「１５７．２．３．０」にマッチする場合には該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＣが実行されることを表している。

【００５２】なお、図１２に示すように、転送先テーブルにおいては、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも上に存在している。そして、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも優先的に適用される。また、各エントリーは、通信装置へ到着したパケットのみに対して適用され、転送のために送出されるパケットに対しては適用されない。

【００５３】以上説明した通信装置の構成をまとめる。図１１に示したインタフェース部は、通信線毎に設けられており、当該通信線から到着するパケットを受信するとともに当該通信線に対してパケットを送出する処理を行う。また、転送先テーブル記憶部は、パケットの送信元アドレスまたは宛先アドレスまたはそれら両方のアドレスのパターンと、該パターンに対応するプログラム

20

（アクティブコード）の情報あるいは該パターンに対応する転送先アドレスの情報とが登録された転送先テーブルを記憶する。また、アクティブネットワーク実行環境は、前記プログラムを予め記憶しているとともに、このプログラムを実行する。また、転送処理部は、通信線から到着した受信パケットを前記インタフェース部から渡された際に、当該受信パケットの送信元アドレスまたは宛先アドレスに基づいて前記転送先テーブルを参照し、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応する転送先アドレスの情報が登録されていた場合には当該受信パケットを所定の転送先アドレスに向けて送出するように当該転送先アドレスに対応したインタフェース部に渡すとともに、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応するプログラムの情報が登録されていた場合には前記アクティブネットワーク実行環境部において当該プログラムを起動させるとともに当該プログラムに当該受信パケットを渡す。

【００５４】次に、本実施形態におけるアクティブコードのセキュリティに関するモデルについて説明する。このセキュリティのモデルは、各々のアクティブコードが、アクティブコードの所有者に関わるパケットのみに対して作用することを保証するためのものである。そのために、このセキュリティのモデルは、公開鍵のインフラストラクチャの存在を前提として、それを利用することとする。

【００５５】図１３は、上記のセキュリティモデルとそのモデルにおける処理の手順を示す概略図である。図１３において、符号７０５１はユーザＡのユーザ端末装置、７０６１は認証局（Certification Authority）装置である。この認証局の機能は、公の機関によって提供されるものであっても良いし、あるいはＩＳＰ（Internet Service Provider,インターネット接続サービス提供者）などによって提供されるものであっても良い。なお、図１３に示す例では、ユーザ端末装置７０５１のＩＰアドレスは「１．２．３．４」である。以下では、ユーザＡが、アクティブコードＡを通信装置７００１に登録するための処理の手順を説明する。なお、以下において、ユーザＡはアクティブコードＡの開発者であっても良いが、その必然性はなく、他の開発者が開発したアクティブコードＡをユーザＡが入手し、それを通信装置７００１に登録するものでも良い。

【００５６】まず（１）で示すように、ユーザＡのユーザ端末装置７０５１は、周知技術を用いて鍵のペアすなわち公開鍵と秘密鍵とを生成する。そして（２）で示すように、ユーザ端末装置７０５１は、上で生成された公開鍵を認証局装置７０６１に登録する。このとき、認証局装置７０６１は、ユーザ端末装置７０５１のＩＰアドレスを検証する。この検証が正しく行なわれると、公開鍵そのものと、ユーザＡを識別するための情報と、ユー

ザ端末装置７０５１のＩＰアドレス「１．２．３．４」が認証局装置７０６１に記憶される。

【００５７】次に（３）で示すように、ユーザ端末装置７０５１は、上で生成された秘密鍵を用いてアクティブコードＡに電子署名する処理を行う。そして（４）で示すように、ユーザ端末装置７０５１は、秘密鍵で署名されたアクティブコードＡを通信装置７００１に登録する処理を行う。

【００５８】これを受けて通信装置７００１は、（５）で示すように、アクティブコードＡの登録を行ったユーザＡの電子証明書を認証局装置７０６１から取得する。この電子証明書には、ユーザＡを識別する情報と、そのＩＰアドレス「１．２．３．４」と、上の（２）において登録された公開鍵そのものとが含まれている。そして（６）で示すように、通信装置７００１は、上記の電子証明書から取り出したユーザＡの公開鍵を用いて、上の（４）において登録されたアクティブコードＡの電子署名を検証する。そして、これが正しく検証された場合には、通信装置７００１は、アクティブコードＡをアクティブネットワーク実行環境に導入する処理を行う。また、これに応じて、転送先テーブルに必要なエントリーが追加される。

【００５９】なお、この（１）および（２）の処理が行われて一旦ユーザＡの公開鍵が認証局装置７０６１に登録されると、ユーザ端末装置７０５１はその公開鍵に対応する秘密鍵を用いてアクティブモジュールをいくつでも通信装置７００１に登録することも可能である。

【００６０】つまり、通信装置７００１は登録部（図示せず）を備えており、この登録部は、ユーザの端末装置から当該ユーザの秘密鍵で電子署名されたプログラムを受信し、当該ユーザの電子証明書を認証局装置から受信し、受信した電子証明書に含まれる当該ユーザの公開鍵を用いて前記電子署名されたプログラムの検証を行い、この検証が成功した場合には当該プログラムに対応するアドレスのパターンと当該プログラムの情報とを前記転送先テーブルに登録し、この検証が失敗した場合には当該プログラムの情報の前記転送先テーブルへの登録は行わないようにするものである。

【００６１】なお、上で説明した通信装置へのアクティブコードの登録の手順が有効に機能するためには、次の２点が前提となる。第１の前提として、ユーザがどの通信装置（ノード）にアクティブコードを登録すれば良いかは事前にわかっている。あるいは、どの通信装置（ノード）にアクティブコードを登録すればよいかがわかるためのディレクトリサービスが提供されている。第２の前提として、通信装置（ノード）は、目的の認証局の公開鍵を事前にオフラインで取得しているか、他の認証局から取得するか、あるいは他の何らかの手段で取得できる。

【００６２】次に、矛盾の解消のための制御について説

明する。ある通信装置（ノード）において、ｎ個のアクティブコードが登録されており、ｉ番目（１≦ｉ≦ｎ）とｊ番目（１≦ｊ≦ｎ）のアクティブコードが、それぞれ集合Ｃ（ｉ）（Ｃ（ｉ）⊆Ａ）と集合Ｃ（ｊ）（Ｃ（ｊ）⊆Ａ）に属するパケットに対するものであると定義されているとき、集合（ｃ（ｉ）∩ｃ（ｊ））が空集合ではないようなｉおよびｊの組み合せ（但しｉ≠ｊ）が存在する場合があり得る。つまり、あるパケットがｉ番目のアクティブコードにもｊ番目のアクティブコードにも適用されるような定義が行われている場合である。このような矛盾は、次の２通りのシナリオのいずれかによって解消することとする。

【００６３】第１の矛盾の解消のシナリオは、パケット（ｓ，ｄ）に関して、

（ｓ∈Ｏ（ｋ）∧ｄ∈Ｏ（ｌ））∧（ｋ≠ｌ）

であるために、

（ｓ，ｄ）∈ｃ（ｉ）∩ｃ（ｊ）

となる場合に関するものである。但し、Ｏ（ｋ）およびＯ（ｌ）は、それぞれユーザｋおよびｌによって所有されるＩＰアドレスの集合である。つまり、あるパケットに関して、送信元のユーザ用のアクティブコードと宛先のユーザ用のアクティブコードとの両方が通信装置に登録されており、そのような通信装置にこのパケット（ｓ，ｄ）が到着した場合である。このような場合には、宛先のユーザのアクティブコードを優先的に適用することが望ましいと考えられる。

【００６４】つまり、転送先テーブルに登録されているパターンに、送信元アドレスのみが指定されていて宛先アドレスが何でもよいとされている第１のエントリーと、宛先アドレスのみが指定されていて送信元アドレスが何でもよいとされている第２のエントリーとが含まれており、受信パケットがこれら第１のエントリーと第２のエントリーとの両方にマッチしたときには、第１のエントリーよりも第２のエントリーを優先させて、当該第２のエントリーのパターンに対応するプログラムを起動するようにする。

【００６５】このように、送信元のユーザのアクティブコードよりも宛先のユーザのアクティブコードを優先させることは、アクティブネットワークの機能を用いてＤｏＳ（分散型ＤｏＳ，Distributed Denial of Service）攻撃を防御するメカニズムを構築する場合に特に重要となる。そのようにすることによって、宛先のユーザつまり被攻撃者となり得る者のアクティブコードが、攻撃者となる可能性があるもののアクティブコードよりも優先されるためである。

【００６６】第２の矛盾の解消のシナリオは、あるパケット（ｓ，ｄ）に関して適用されるべき２つ以上のアクティブコードが同一のユーザによって登録されている場合に関するものである。このような場合には、該当するアクティブコードのうちの最も古く登録されたものが、

他のものよりも優先的に適用されるようにすることが望ましいと考えられる。こうすることにより、ユーザが新しいアクティブコードを登録しようとする際には、新しいアクティブコードを有効にするために事前に古いアクティブコードを削除することが保証されるからである。

【００６７】次に、これまでに述べたようなアクティブネットワークのノードとして機能する通信装置のインプリメンテーションの例について説明する。図１４は、Ｌｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行う通信装置を実現した場合の概略図である。

【００６８】図１４に示す例では、専用のＩＰスタックを処理（process）の一部として構築している。これによって、図１２に示したような転送先テーブルを実現し、実行環境（アクティブネットワーク実行環境）からこの転送先テーブルにエントリーの追加や削除を行えるようにしている。また、これに伴い、カーネル（kernel）内のＩＰスタックは不要となるため、カーネルにおけるルーティングを不活性化している。そして、到着パケットのコピーがデータリンク部分から作成され、そのパケットがライブラリｌｉｂｐｃａｐを通してＪａｖａ（登録商標）仮想マシンで補足できるようにしている。

【００６９】処理の一部として構築した専用のＩＰスタックは、アクティブパケット、つまり転送先テーブル上での所定の定義にマッチするＩＰアドレス（宛先ＩＰアドレス、送信元ＩＰアドレス、あるいはそれらの組み合せ）を有するパケットは、実行環境上で起動されるアクティブコードに対して渡される。一方、アクティブパケット以外の通常のパケットは、カーネルにおけるＩＰスタックと同様の方法で隣接する通信装置等へ向けた転送が行われる。アクティブパケットであれ通常パケットであれ、この通信装置から送出されるすべてのパケットは、ライブラリｌｉｂｎｅｔを通して送出される。こうすることにより、各々処理されたパケットのヘッダに記録された送信元アドレスは、元々の送信元アドレスのままの状態で、ネットワークに送出されることとなる。

【００７０】また、標準のＪａｖａ（登録商標）のＡＰＩ（アプリケーションプログラムインタフェース）である「java.security」を用いることによってセキュリティモデルをインプリメンテーションすることが可能である。この標準ＡＰＩは、セキュリティモデルを構築するために必要な機能のほとんどを提供している。また、証明書のための形式としては「Ｘ．５０９」証明書形式を用いることが可能であり、アクティブコードの所有者のＩＰアドレスを「Ｘ．５０９」の識別名（ＤＮ，distinguished name）の一部に含めることにより、本実施形態のセキュリティモデルを実現することができる。

【００７１】なお、言うまでもなく、上記インプリメンテーションではコンピュータシステムを用いることによってアクティブネットワーク実行環境を備えた通信装置を構築している。そして、上述した一連の処理、すなわち到着パケットの複製の作成とその捕捉や、転送先テーブルを参照しながらのアクティブパケットおよび通常パケットの転送の処理や、アクティブネットワーク実行環境上でのアクティブコードの起動とその処理の実行や、処理されたパケットのネットワークへの送出などの各処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。

【００７２】なお、上述した各コンピュータプログラムは、コンピュータ読取可能な記録媒体に記録されており、通信装置等に搭載されたＣＰＵ（中央処理装置）がこの記録媒体からコンピュータプログラムを読み取って、攻撃防御あるいはサービスモジュール提供等のための各処理を実行する。また、「コンピュータ読み取り可能な記録媒体」とは、磁気ディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

【００７３】また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されても良い。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

【００７４】また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムに既に記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

【００７５】また、下流のゲート通信装置から上流の通信装置へのデータの送信は、アクティブネットワークの使用に限定するものではなく、任意の通信プロトコルの使用が可能である。

【００７６】また、ゲート装置及び通信装置はゲートウェイやルータに限られるものではなく、ブリッジ、イーサネット（登録商標）、インタフェース変換装置など、ＩＰアドレスを持つ任意の通信ノードであっても良い。

【００７７】以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

25

【００７８】

【発明の効果】以上説明したように、ネットワーク上の各通信装置はＤＤｏＳ攻撃の被攻撃者が指定した属性によって検出した攻撃容疑トラヒックの容疑シグネチャを再帰的に通知することが可能になるため、ネットワーク全体で被攻撃者の要求する攻撃容疑トラヒックの伝送帯域を制限することが可能になるとともに、早期にネットワークの輻輳を改善することが可能となる。そして、ネットワーク上のそれぞれの通信装置は、攻撃容疑トラヒックを監視して攻撃パケットを特定することにより攻撃パケットのみを更に制限することが可能になるため、正規ユーザのパケットが誤って攻撃パケットとして分類され、破棄される可能性を低くするとともに、攻撃元に最も近い最上流の通信装置において攻撃を防御する、すなわちＤＤｏＳ攻撃の通信パケットを破棄することでネットワークの伝送帯域の浪費を防ぐことができる。

【００７９】また、ネットワークの各通信装置はＤＤｏＳ攻撃の被攻撃者が指定した正規シグネチャを再帰的に通知することで、各通信装置は被攻撃者が指定した正規ユーザの通信トラヒックの伝送帯域の制限を解除することが可能になる。従って、ＤＤｏＳ攻撃の通信パケットを破棄しながらも、被攻撃者の指定するサービスポリシーを反映して、ネットワーク上の正規利用者のトラヒックの疎通を確保することが可能となり、ネットワーク全体への悪影響を抑制することができる。

【００８０】また、例えばインターネットのように、本来攻撃防御の機能を備えていないネットワークであっても、本発明を適用することによって攻撃に対する効果的な防御が可能になる。また本発明を用いた場合、攻撃者が直接接続されているネットワークの管理者が何らかの対処をする必要がなく、攻撃を受けている装置が接続されているネットワーク側の対処によって自動的に防御機能が起動され攻撃を防ぐことができるようになる。

【図面の簡単な説明】

【図１】　本発明の一実施の形態を適用できるネットワークの構成図である。

【図２】　同実施の形態による攻撃容疑検出条件の設定の例である。

【図３】　同実施の形態による正規条件の設定の例である。

【図４】　同実施の形態による不正トラヒック検出条件の設定の例である。

【図５】　同実施の形態によるゲート装置２００１及び通信装置２００２～２００６が備える帯域制御モデルである。

【図６】　同実施の形態によるフィルタ２０２１における分類アルゴリズムである。

26

【図７】　同実施の形態によるゲート装置２００１の攻撃容疑パケット検出時の動作を示すフローチャートである。

【図８】　同実施の形態による通信装置２００２、２００３のシグネチャ受信時の動作を示すフローチャートである。

【図９】　同実施の形態によるゲート装置２００１及び通信装置２００２～２００６の不正トラヒック検出時の動作を示すフローチャートである。

【図１０】　同実施の形態を実行できるアクティブネットワークが前提とするネットワークの構成である。

【図１１】　同実施の形態を実行できるアクティブネットワークによる通信装置内部の構成を示すブロック図である。

【図１２】　同実施の形態を実行できるアクティブネットワークによる転送先テーブル記憶部に記憶されている転送先テーブルの一例を示す概略図である。

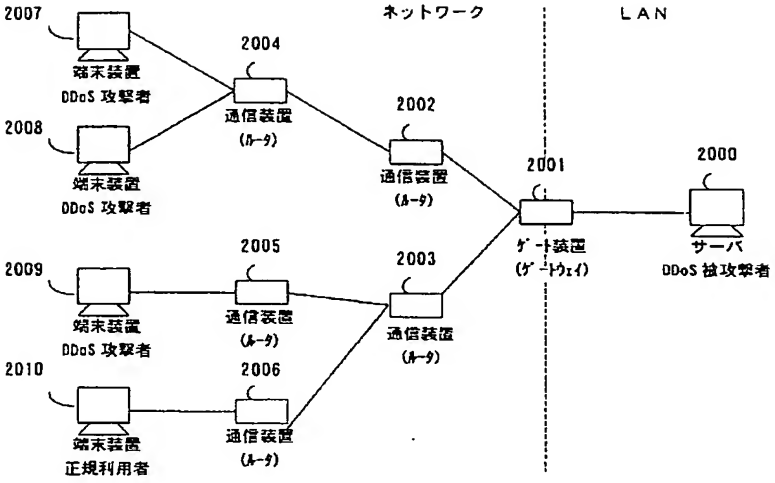
【図１３】　同実施の形態を実行できるアクティブネットワークによるセキュリティモデルとそのモデルにおける処理の手順を示す概略図である。

【図１４】　同実施の形態を実行できるアクティブネットワークの通信装置をＬｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行うように実現した場合の概略図である。

【符号の説明】

２０００…サーバ
２００１…ゲート装置
２００２～２００６…通信装置
２００７～２０１０…端末装置
２０２１…フィルタ
２０２２…正規クラス
２０２３…正規キュー
２０２４…不正クラス
２０２５…不正キュー
２０２６…容疑クラス
２０２７…容疑キュー
７０００…ユーザのコンピュータ
７００１…通信装置
７０１０…アクティブネットワーク実行環境
７０１１…コード実行部
７０１２…コード記憶部
７０２１…転送処理部
７０２２…転送先テーブル記憶部
７０２３ａ、７０２３ｂ…インタフェース部
７０２４ａ、７０２４ｂ…通信線
７０５１…ユーザ端末装置
７０６１…認証局装置

【図１】



【図２】

番号	検出属性	検出閾値	検出間隔
1	(Dst=192.168.1.1/32, Protocol=TCP, Port=80)	500Kbps	10 秒
2	(Dst=192.168.1.2/32, Protocol=UDP)	300Kbps	10 秒
3	(Dst=192.168.1.0/24)	1Mbps	20 秒

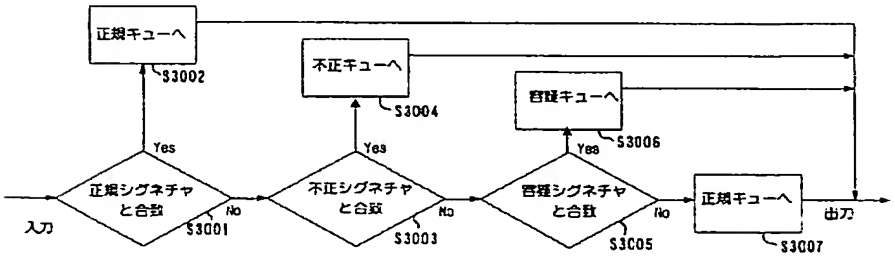
【図３】

番号	検出属性
1	(Src=172.16.10.0/24)
2	(TOS=0x01)

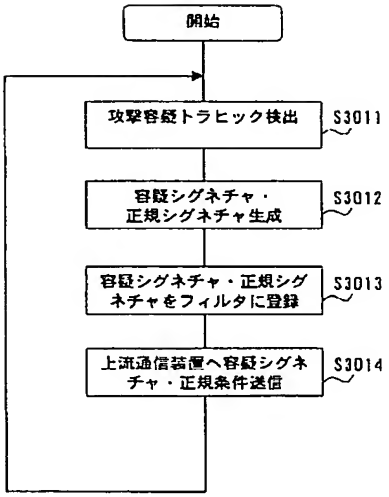
【図４】

番号	不正トラヒック条件
1	T1 Kbps 以上のパケットが S1 秒以上連続送信されている
2	T2 Kbps 以上の ICMP/Echo Reply パケットが S2 秒以上連続送信されている
3	T3 Kbps 以上のフラグメントパケットが S3 秒以上連続送信されている

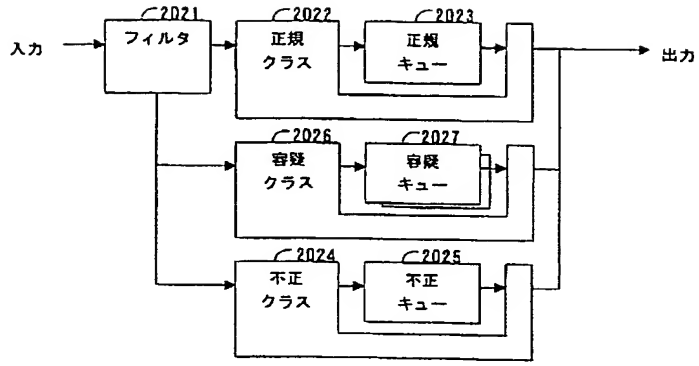
【図６】



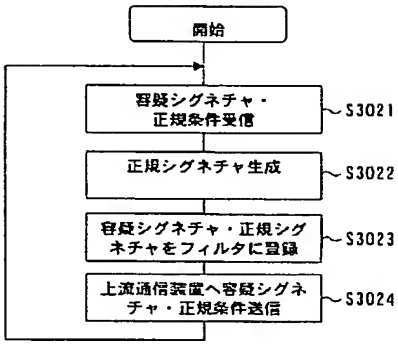
【図７】



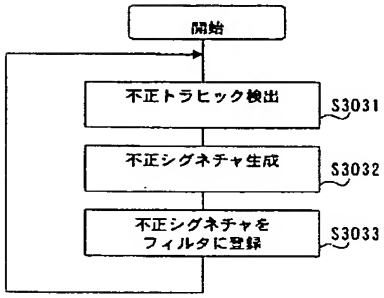
【図５】



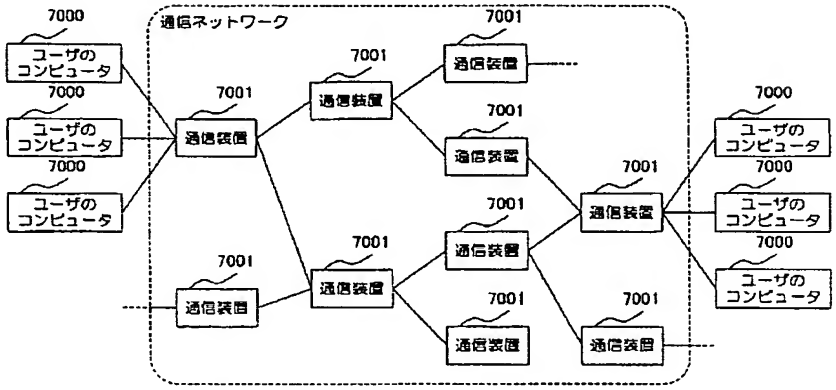
【図８】



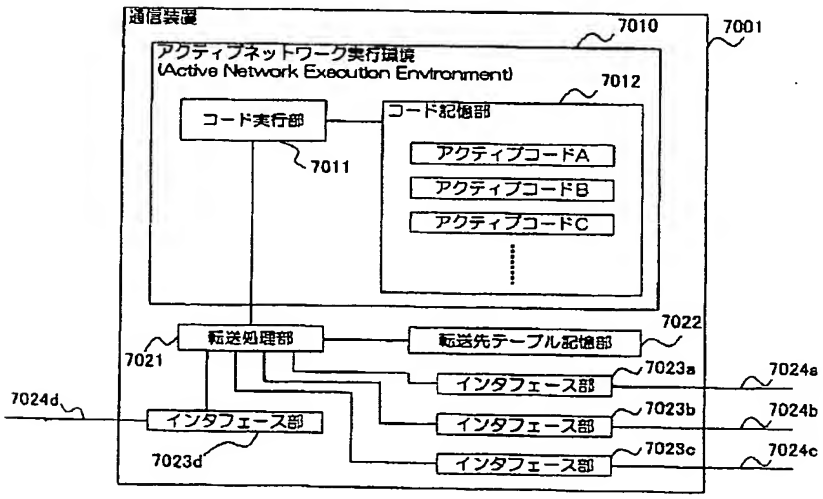
【図９】



【図１０】



【図１１】

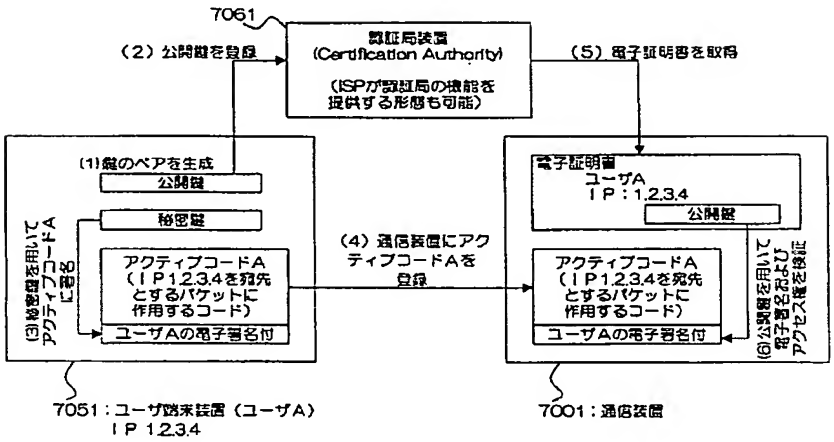


【図１２】

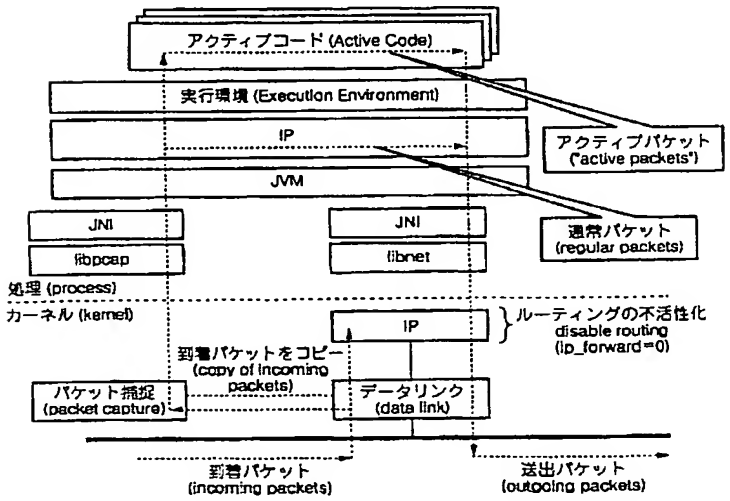
転送先テーブル

タイプ (Type)	宛先アドレス (Destination)	送信元アドレス (Source)	転送先 (Send to)
アクティブ (Active)	1.2.3.4	Any	アクティブコードA
アクティブ	10.50.0.0	11.12.13.14	アクティブコードB
アクティブ	Any	157.2.3.0	アクティブコードC
通常 (Regular)	1.2.0.0	N/A	29.15.20.1
通常	11.20.0.0	N/A	109.1.1.10
通常	199.1.1.0	N/A	120.0.0.1
⋮	⋮	⋮	⋮

【図１３】



【図１４】



フロントページの続き

(72)発明者　冨士　仁
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5K030 GA13 GA15 HA08 HB14 KA06 KX24 KX30 LC15
5K033 AA05 AA08 CB06 CB08 DA16 DB19 DB20 EC03